

**TO: Clerk's Office**  
**UNITED STATES DISTRICT COURT**  
**EASTERN DISTRICT OF NEW YORK**



**APPLICATION FOR LEAVE**  
**TO FILE DOCUMENT UNDER SEAL**

\*\*\*\*\*  
UNITED STATES OF AMERICA

- v -

JULES MEFRE,  
also known as "John Frisk"

23-MJ-799

Docket Number

\*\*\*\*\*

SUBMITTED BY: Plaintiff \_\_\_ Defendant \_\_\_ DOJ ☒  
Name: Andrew D. Reich  
Firm Name: USAO EDNY  
Address: 271-A Cadman Plaza East  
Brooklyn NY 11201  
Phone Number: 718-254-6452  
E-Mail Address: andrew.reich@usdoj.gov

INDICATE UPON THE PUBLIC DOCKET SHEET: YES \_\_\_ NO ☒

If yes, state description of document to be entered on docket sheet:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

**MANDATORY CERTIFICATION OF SERVICE:**

A.) \_\_\_ A copy of this application either has been or will be promptly served upon all parties to this action, B.) \_\_\_ Service is excused by 31 U.S.C. 3730(b), or by the following other statute or regulation: \_\_\_\_\_; or C.) ☒ This is a criminal document submitted, and flight public safety, or security are significant concerns. (Check one)

09/07/2023  
DATE

SIGNATURE

**A) If pursuant to a prior Court Order:**

Docket Number of Case in Which Entered: \_\_\_\_\_

Judge/Magistrate Judge: \_\_\_\_\_

Date Entered: \_\_\_\_\_

**B) If a new application,** the statute, regulation, or other legal basis that authorizes filing under seal

Ongoing criminal investigation: \_\_\_\_\_

**ORDERED SEALED AND PLACED IN THE CLERK'S OFFICE,  
AND MAY NOT BE UNSEALED UNLESS ORDERED BY  
THE COURT.**

DATED: Brooklyn, NEW YORK  
09/07/2023

s/ James R. Cho

**U.S. MAGISTRATE JUDGE**

RECEIVED IN CLERK'S OFFICE 09/07/2023

DATE

DCP:ADR  
F. #2021R00699

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK

----- X

UNITED STATES OF AMERICA

- against -

JULES MEFRE,  
also known as "John Frisk,"

Defendant.

----- X

EASTERN DISTRICT OF NEW YORK, SS:

JONATHAN PECK, being duly sworn, deposes and states that he is a Special Agent with the United States Secret Service, duly appointed according to law and acting as such.

In or about and between January 2023 and August 2023, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant JULES MEFRE, also known as "John Frisk," together with others, did knowingly and intentionally engage in one or more monetary transactions, in and affecting interstate and foreign commerce, by, through and to one or more financial institutions, in criminally derived property that was of a value greater than \$10,000 and that was derived from specified unlawful activity, to wit: wire fraud and bank fraud, in violation of Title 18, United States Code, Sections 1343 and 1344, respectively, knowing that the property involved in such monetary transactions represented the proceeds of some form of unlawful activity.

(Title 18, United States Code, Section 1957(a))

**To Be Filed Under Seal**

**COMPLAINT AND**  
**AFFIDAVIT IN SUPPORT**  
**OF AN APPLICATION FOR**  
**AN ARREST WARRANT**

(18 U.S.C. § 1957(a))

Case No. 23-MJ-799

The source of your deponent's information and the grounds for his belief are as follows:<sup>1</sup>

1. I am a Special Agent with the United States Secret Service ("USSS") and have been involved in the investigation of numerous cases involving wire fraud, bank fraud and money laundering. I am familiar with the facts and circumstances set forth below from my participation in the investigation, my review of the investigative file, interviews with witnesses and victims, and reports of other law enforcement officers involved in the investigation.

2. In or about and between January and August 2023, the defendant JULES MEFRE knowingly received proceeds from a series of fraudulent business email compromise ("BEC") schemes that resulted in more than two million dollars in losses by victims in the United States and abroad.<sup>2</sup> As part of the schemes, employees of victim-companies and other victim-entities received fraudulent emails purporting to be from legitimate vendors or other business partners of those companies and entities directing them to transfer funds to specified bank accounts. The fraudulent email accounts that contacted the employees closely resembled, but were slightly different from, the email addresses of the legitimate parties to the transaction. After the employees executed the wires in accordance

---

<sup>1</sup> Because the purpose of this Complaint is to set forth only those facts necessary to establish probable cause to arrest, I have not described all the relevant facts and circumstances of which I am aware.

<sup>2</sup> A BEC scheme is a form of cyber-enabled financial fraud. In a typical BEC scheme, a malicious actor compromises legitimate business email accounts through computer intrusion techniques or social engineering and uses those accounts to cause the unauthorized transfer of funds. Techniques for perpetrating these schemes include identity theft, spoofing of emails and websites and the use of malware.

with the fraudulent instructions, the transferred funds were misappropriated from the victim-companies and other victim-entities and sent to and through accounts controlled by MEFRE.

3. As one example of the BEC schemes, in or about April 2023, a regional transit services commission in Alberta, Canada (“Victim-1”), the identity of which is known to your deponent, received an email from one of its legitimate vendors, a manufacturer of transit buses (“Vendor-1”), the identity of which is known to your deponent, regarding payment on two outstanding invoices. The domain for the sender’s email address bore Vendor-1’s name. On or about May 1, 2023, Victim-1 received another email, purporting to be from Vendor-1, attaching “updated” invoices that instructed Victim-1 to send payment to a specified bank account. However, the May 1, 2023 email was fraudulent and was not sent by Vendor-1. Instead, it was sent from an email account with a domain name that was a misspelled version of Vendor-1’s name. Specifically, the domain for this email address had an added “z” at the end. Records obtained by the USSS indicate that the domain was created on or about April 28, 2023, days before the fraudulent email was sent. On or about May 5, 2023, as a result of the fraudulent email, Victim-1 wired approximately \$1,519,000 to the specified account.

4. The account specified in the fraudulent email to Victim-1, and to which Victim-1 wired the funds, was an account at a financial institution headquartered in New York, New York (“Financial Institution-1”), the identity of which is known to your deponent, belonging to an entity called “Frisk Logistics LLC” (the “Financial Institution-1 Account”). The Financial Institution-1 Account was opened on or about January 30, 2023 and had as its signatory “John Frisk,” with a social security number ending in -0969. The Financial Institution-1 Account also listed a Georgia state driver’s license bearing the name “John

Frisk” with a license number ending in -0909 and an email address of johnfrisk1983@gmail.com. As explained further below, “John Frisk” is a fraudulent identity used by the defendant JULES MEFRE. Information obtained from law enforcement databases revealed that the -0909 driver’s license number is associated with an active Georgia state driver’s license issued to an individual by a different name. The mailing address listed for the account was an address in Chicago, Illinois.<sup>3</sup>

5. On or about May 8, 2023, Financial Institution-1 informed Victim-1 that it had frozen the May 5, 2023 transaction due to fraud concerns.

6. As another example of the BEC schemes, on or about August 14, 2023, a ranch in Ottawa, Kansas (“Victim-2”), the identity of which is known to your deponent, received an email purporting to be from its legitimate vendor, a supplier of crop treatments (“Vendor-2”), the identity of which is known to your deponent, instructing Victim-2 to make certain outstanding payments to a specified bank account. However, the email was fraudulent and was not sent by Vendor-2. Instead, it was sent from an email account with a domain name that was a misspelled version of Vendor-2’s name. Specifically, the domain for the email address swapped the order of two of the letters in Vendor-2’s name. On or about August 14, 2023, as a result of the fraudulent email, Victim-2 wired approximately \$632,400.60 to the specified account.

7. The account specified in the fraudulent email to Victim-2, and to which Victim-2 wired the funds, was an account at a financial institution headquartered in New

---

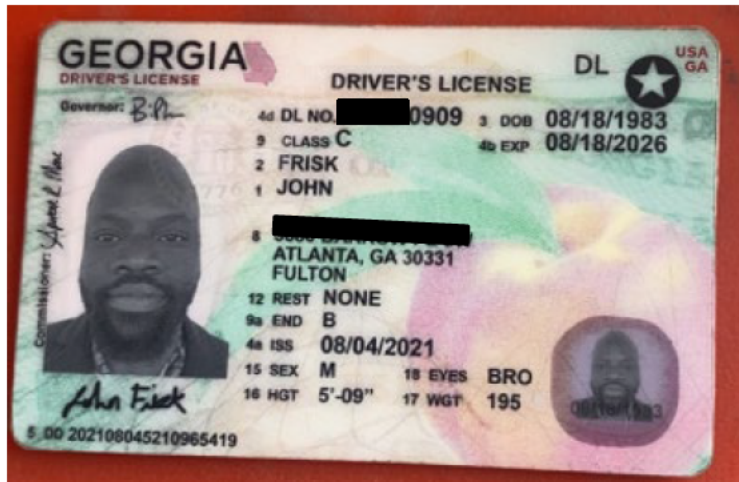
<sup>3</sup> I am aware based on documents obtained by USSS and physical surveillance conducted by USSS as recently as August 2023 that MEFRE resides in Chicago, Illinois.

York, New York (“Financial Institution-2”), the identity of which is known to your deponent, also belonging to “Frisk Logistics LLC” (the “Financial Institution-2 Account”). The Financial Institution-2 Account was opened in or about February 2023. The signatory on the Financial Institution-2 Account was “John Frisk” and it was opened using the Georgia state driver’s license bearing that name and a license number ending in -0909. The email addresses listed for the Financial Institution-2 Account were johnfrisk1983@gmail.com and johnfrisk44@gmail.com. The mailing address listed for the account was an address in Chicago, Illinois.

8. According to information obtained from Financial Institution-2, shortly after the Victim-2 funds were received into the Financial Institution-2 Account on or about August 14, 2023, the account funds were substantially depleted through a series of wire transfers to accounts at other financial institutions, including, for example, a wire transfer of approximately \$250,000 on or about August 15, 2023 to an account at a financial institution whose identity is known to your deponent (“Financial Institution-3”). Furthermore, according to information obtained by Financial Institution-2, as of September 2023, the Financial Institution-2 Account was frozen as a result of suspected fraud.

9. Both the Financial Institution-1 Account and the Financial Institution-2 Account (together, the “Accounts”) are controlled by the defendant JULES MEFRE. A review of a mobile phone used by MEFRE (the “Phone”), which MEFRE provided to USSS agents pursuant to a judicially-authorized search warrant, revealed evidence linking MEFRE to the fraudulent “John Frisk” identity and to the Accounts. Specifically, MEFRE’s phone contained an image of a Georgia state driver’s license bearing the name “John Frisk” and

license number ending in -0909, as described above and as depicted below. Metadata associated with the image indicates that it was photographed using the Phone.



10. The Phone contained additional evidence linking the defendant JULES MEFRE to the Accounts. With respect to the Financial Institution-1 Account, among other things, the Phone contained: (i) a message sent by MEFRE on or about March 13, 2023 to an unknown user (“User-1”) on an encrypted messaging platform (“Platform-1”) with account information pertaining to the Financial Institution-1 Account; and (ii) a video sent by MEFRE on or about August 5, 2023 to User-1 depicting a successful login to a Financial Institution-1 online banking account using the username johnfrisk1983.<sup>4</sup>

11. With respect to the Financial Institution-2 Account, among other things, the Phone contained: (i) a message sent by the defendant JULES MEFRE on or about July 17, 2023 to another unknown user on Platform-1 (“User-2”) with account information pertaining to the Financial Institution-2 Account; (ii) an image sent by MEFRE to User-1 on

<sup>4</sup> In the video, after the password is successfully entered, a message appears on the screen indicating that the account has been locked “due to suspicious activity.”



or about August 8, 2023 depicting a phone logged into an online banking account for the Financial Institution-2 Account (the last four digits of the account number are visible in the image); and (iii) an image, with metadata indicating it was photographed by the Phone, depicting a computer screen logged into the online banking account for the Financial Institution-2 Account (with account number fully visible) on the “Recent Account Activity” page, showing receipt of an August 14, 2023 wire from Victim-2 for \$632,400.60, as described above and as depicted below.

Beneficiary Information	Amount	Date / Time	Originating Information	Reference Numbers
Account [REDACTED]	\$632,400.60	Date Posted: [REDACTED]	RANCH INC	Fed Ref# [REDACTED]
FRISK LOGISTICS LLC		08/14/23	Bank	20230814MMQFMPMT00016920230814B1Q8021R033244
[REDACTED]		Received: [REDACTED]		Global Ref# [REDACTED]
		08/14/23 13:38:48		F013226081DC01

Generated August 16 2023 at 10:17:09

12. The Phone also contained a series of messages with a third unknown user on Platform-1 (“User-3”) discussing the sale of false identification documents, further demonstrating the defendant JULES MEFRE’s use of the fraudulent “John Frisk” identity. On or about April 8, 2023, MEFRE messaged User-3, “Send me all the stuff you do and the prices.” That same day, User-3 replied with an extensive list of identification documents and prices, including: “Ssn plain \$150, with real rose gold \$500,” “Bank Statements \$100 a page,” “Utility bill \$100,” “Passport card \$2k,” “Green Card \$20k,” “Birth certificate \$250,”



“Car Title \$1,000 IL,” “Certificate of incorporation \$200,” “W2’s \$200 other tax forms \$125.” MEFRE replied, “Thank you brother.”

13. On or about June 27, 2023, the defendant JULES MEFRE messaged User-3, “Please I need Ssn card.” On or about June 29, 2023, User-3 responded, “Hey I’m available.” That same day, MEFRE messaged User-3, “Okay let me send details.” On or about July 3, 2023, MEFRE messaged User-3, “Name: JOHN FRISK” and “SSN:” followed by the social security number ending in -0969 used to open the Financial Institution-1 Account, as described above.

WHEREFORE, your deponent respectfully requests that the defendant JULES MEFRE be dealt with according to law. Because public filing of this document could result in a risk of flight by MEFRE, as well as jeopardize the government’s ongoing investigation, your deponent respectfully requests that this complaint, as well as any arrest warrant issued in connection with this complaint, be filed under seal.

/s/ Jonathan Peck  
\_\_\_\_\_  
JONATHAN PECK  
Special Agent  
United States Secret Service

Sworn to before me by telephone this  
7th day of September, 2023

s/ James R. Cho  
\_\_\_\_\_  
THE HONORABLE JAMES R. CHO  
UNITED STATES MAGISTRATE JUDGE  
EASTERN DISTRICT OF NEW YORK

## UNITED STATES DISTRICT COURT

for the

Eastern District of New York

United States of America

v.

JULES MEFRE,  
also known as "John Frisk,"

Case No. 23-MJ-799

---

Defendant

## ARREST WARRANT

To: Any authorized law enforcement officer

**YOU ARE COMMANDED** to arrest and bring before a United States magistrate judge without unnecessary delay  
 (name of person to be arrested) Jules Mefre, also known as "John Frisk",  
 who is accused of an offense or violation based on the following document filed with the court:

☐ Indictment    ☐ Superseding Indictment    ☐ Information    ☐ Superseding Information    ☒ Complaint  
☐ Probation Violation Petition    ☐ Supervised Release Violation Petition    ☐ Violation Notice    ☐ Order of the Court

This offense is briefly described as follows:

18 U.S.C. § 1957(a) (engaging in monetary transactions in property derived from specified unlawful activity)

Date: 09/07/2023

s/ James R. Cho

---

Issuing officer's signatureCity and state: Brooklyn, New York

Hon. James R. Cho

---

Printed name and title

## Return

This warrant was received on (date) \_\_\_\_\_, and the person was arrested on (date) \_\_\_\_\_  
 at (city and state) \_\_\_\_\_.

Date: \_\_\_\_\_

---

Arresting officer's signature

---

Printed name and title

**This second page contains personal identifiers provided for law-enforcement use only  
and therefore should not be filed in court with the executed warrant unless under seal.**

*(Not for Public Disclosure)*

Name of defendant/offender: \_\_\_\_\_

Known aliases: \_\_\_\_\_

Last known residence: \_\_\_\_\_

Prior addresses to which defendant/offender may still have ties: \_\_\_\_\_

Last known employment: \_\_\_\_\_

Last known telephone numbers: \_\_\_\_\_

Place of birth: \_\_\_\_\_

Date of birth: \_\_\_\_\_

Social Security number: \_\_\_\_\_

Height: \_\_\_\_\_ Weight: \_\_\_\_\_

Sex: \_\_\_\_\_ Race: \_\_\_\_\_

Hair: \_\_\_\_\_ Eyes: \_\_\_\_\_

Scars, tattoos, other distinguishing marks: \_\_\_\_\_

History of violence, weapons, drug use: \_\_\_\_\_

Known family, friends, and other associates (*name, relation, address, phone number*): \_\_\_\_\_

FBI number: \_\_\_\_\_

Complete description of auto: \_\_\_\_\_

Investigative agency and address: \_\_\_\_\_

Name and telephone numbers (office and cell) of pretrial services or probation officer (*if applicable*): \_\_\_\_\_

Date of last contact with pretrial services or probation officer (*if applicable*): \_\_\_\_\_